

On Shifted Eisenstein Polynomials

RANDELL HEYMAN

Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
`randell@unsw.com.au`

IGOR E. SHPARLINSKI

Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
`igor.shparlinski@mq.edu.au`

Abstract

We study polynomials with integer coefficients which become Eisenstein polynomials after the additive shift of a variable. We call such polynomials *shifted Eisenstein polynomials*. We determine an upper bound on the maximum shift that is needed given a shifted Eisenstein polynomial and also provide a lower bound on the density of shifted Eisenstein polynomials, which is strictly greater than the density of classical Eisenstein polynomials. We also show that the number of irreducible degree n polynomials that are not shifted Eisenstein polynomials is infinite. We conclude with some numerical results on the densities of shifted Eisenstein polynomials.

1 Introduction

It is well known that almost all polynomials in rather general families of $\mathbb{Z}[x]$ are irreducible, see [3, 12] and references therein. There are also known polynomial time irreducibility tests and polynomial time factoring algorithms, see for example [7]. However, it is always interesting to study large classes of polynomials that are known to be irreducible.

Thus, we recall that

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x] \quad (1)$$

is called an *Eisenstein polynomial*, or is said to be *irreducible by Eisenstein* if for some prime p we have

- (i) $p \mid a_i$ for $i = 0, \dots, n-1$,
- (ii) $p^2 \nmid a_0$,
- (iii) $p \nmid a_n$.

We sometimes say that f is *irreducible by Eisenstein with respect to prime p* if p is one such prime that satisfies the conditions (i), (ii) and (iii) above (see [2] regarding the early history of the irreducibility criterion).

Recently, motivated by a question of Dobbs and Johnson [4] several statistical results about the distribution of Eisenstein polynomials have been obtained. Dubickas [5] has found the asymptotic density for *monic* polynomials f of a given degree $\deg f = n$ and growing height

$$H(f) = \max_{i=0, \dots, n} |a_i|. \quad (2)$$

The authors [6] have improved the error term in the asymptotic formula of [5] and also calculated the density of general Eisenstein polynomials.

Clearly the irreducibility of polynomials is preserved under shifting of the argument by a constant. Thus it makes sense to investigate polynomials which become Eisenstein polynomials after shifting the argument. More precisely, here we study polynomials $f(x) \in \mathbb{Z}[x]$ for which there exists an integer s such that $f(x+s)$ is an Eisenstein polynomial. We call such $f(x) \in \mathbb{Z}[x]$ a *shifted Eisenstein polynomial*. We call the corresponding s an *Eisenstein shift of f with respect to p* .

For example, for $f(x) = x^2 + 4x + 5$, it is easy to see that $s = -1$ is an Eisenstein shift with respect to $p = 2$.

Here we estimate the smallest possible s which transfers a shifted Eisenstein polynomial $f(x)$ into an Eisenstein polynomial $f(x+s)$. We also estimate the density of shifted Eisenstein polynomials and show that it is strictly greater than the density of Eisenstein polynomials. On the other hand, we show that there are irreducible polynomials that are not shifted Eisenstein polynomials.

More precisely, let \mathcal{I}_n , \mathcal{E}_n and $\overline{\mathcal{E}}_n$ denote the set of irreducible, Eisenstein and shifted Eisenstein polynomials, of degree n over the integers.

Trivially,

$$\mathcal{E}_n \subseteq \overline{\mathcal{E}}_n \subseteq \mathcal{I}_n.$$

We show that all inclusions are proper and that $\overline{\mathcal{E}}_n \setminus \mathcal{E}_n$ is quite “massive”.

2 Notation

We define $\mathcal{I}_n(H)$, $\mathcal{E}_n(H)$ and $\overline{\mathcal{E}}_n(H)$ as the subsets of \mathcal{I}_n , \mathcal{E}_n and $\overline{\mathcal{E}}_n$, respectively, consisting of polynomials of height at most H (where the height of a polynomial (1) is given by (2)).

For any integer $n \geq 1$, let $\omega(n)$ be the number of distinct prime factors and let $\varphi(n)$ be the Euler function of n (we also set $\omega(1) = 0$).

We also use μ to denote the Möbius function, that is,

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{if } n \text{ is square free,} \\ 0 & \text{if } n \text{ otherwise.} \end{cases}$$

Finally, we denote the discriminant of the function f by $D(f)$.

The letters p and q , with or witho

3 A bound on Eisenstein shifts via the discriminant

It is natural to seek a bound on the largest shift required to find a shift if it exists. In fact, for any polynomial, there is a link between the maximum shift that could determine irreducibility and the discriminant.

The following result is well-known and in fact in wider generality, can be proven by the theory of Newton polygons. Here we give a concise elementary proof.

Lemma 1. *Suppose $f \in \mathbb{Z}[x]$ is of degree n . If $f(x)$ is a shifted Eisenstein polynomial then there exists a prime p with $p^{n-1} \mid D(f)$ and $f(x+s)$ is irreducible by Eisenstein for some $0 \leq s < q$, where q is the largest of such primes.*

Proof. Since $f(x)$ is a shifted Eisenstein polynomial there exists an integer t and a prime p such that $f(x+t)$ is irreducible by Eisenstein with respect to p .

Recall that the discriminant of a n degree polynomial can be expressed as the determinant of the $2n-1$ by $2n-1$ Sylvester matrix. Using the Leibniz formula to express the determinant, and examining each summand, it immediately follows that $p^{n-1} \mid D(f(x+t))$. Also, the difference of any two roots of a polynomial is unchanged by increasing both roots by any integer u . So, using the definition of the discriminant, we get $D(f(x)) = D(f(x+u))$ for any integer u . So it follows that $p^{n-1} \mid D(f(x))$.

Furthermore, by expanding $f(x+t+kp)$ for an arbitrary integer k and examining the divisibility of coefficients, it follows that if $f(x+t)$ is Eisenstein with respect to prime q then so too is $f(x+t+kp)$.

By appropriate choice of k we can therefore find an integer s with

$$0 \leq s < p \leq \max\{q \text{ prime} : q^{n-1} \mid D(f)\}$$

such that the polynomial $f(x+s)$ is irreducible by Eisenstein. \square

We also recall a classical bound of Mahler [8] on the discriminant of polynomials over \mathbb{Z} .

For $f(x)$ of the form (1) we define the *length* $L(f) = |a_0| + |a_1| + \dots + |a_n|$.

Lemma 2. *Suppose $f \in \mathbb{Z}[x]$ is of degree n . Then*

$$|D(f)| \leq n^n L(f)^{2n-2}.$$

Combining Lemmas 1 and 2 we derive:

Theorem 3. *Suppose $f(x) \in \mathbb{Z}[x]$. If $f(x+s)$ is not irreducible by Eisenstein for all s with*

$$0 \leq s \leq n^{n/(n-1)} L(f)^2,$$

then f is not a shifted Eisenstein polynomial.

We also remark that the shift s which makes $f(x+s)$ irreducible by Eisenstein with respect to prime p satisfies $f(s) \equiv 0 \pmod{p}$, which can further reduce the number of trials (however a direct irreducibility testing via the classical algorithm of Lenstra, Lenstra and Lovász [7] is still much more efficient).

4 Density of shifted Eisenstein polynomials

In this section we show that as polynomial height grows, the density of polynomials that are irreducible by Eisenstein shifting is strictly larger than the density of polynomials that are irreducible by Eisenstein. We start by calculating a maximum height for $f(x)$ such that $f(x+1)$ is of height at most H .

Lemma 4. *For $f \in \mathbb{Z}[x]$ of degree n , we denote $f_{+1}(x) = f(x+1)$. Then $H(f_{+1}) \leq 2^n H(f)$.*

Proof. Let $f(x)$ be of the form (1). For $i = 0, \dots, n$, the absolute value of the coefficient of x^{n-i} in f_{+1} can be estimated as

$$\sum_{0 \leq j \leq i} \binom{n-j}{i-j} |a_{n-j}| \leq 2^n H(f),$$

as required. \square

We also need the number of polynomials, of given degree and maximum height, that are irreducible by Eisenstein. Let

$$\rho_n = 1 - \prod_p \left(1 - \frac{(p-1)^2}{p^{n+2}} \right). \quad (3)$$

In [6] we prove the following result.

Lemma 5. *We have,*

$$\#\mathcal{E}_n(H) = \rho_n 2^{n+1} H^{n+1} + \begin{cases} O(H^n), & \text{if } n > 2, \\ O(H^2(\log H)^2), & \text{if } n = 2. \end{cases}$$

We also require the following two simple statements.

Lemma 6. *Suppose that $f(x)$ is irreducible by Eisenstein with respect to prime p . Then $f(x+1)$ is not irreducible by Eisenstein with respect to p .*

Proof. Let

$$f(x) = \sum_{i=0}^n a_i x^i \in \mathcal{E}_n$$

be irreducible by Eisenstein with respect to prime p . The coefficient of x^0 in $f(x+1)$ is $a_n + a_{n-1} + \dots + a_1 + a_0$, which is clearly not divisible by p . So $f(x+1)$ is not irreducible by Eisenstein with respect to p . \square

Let

$$\tau_n = \left(\sum_p \frac{(p-1)^2}{p^{n+2}} \right)^2 - \sum_p \frac{(p-1)^4}{p^{2n+4}} \quad (4)$$

Lemma 7. *Let*

$$\mathcal{F}_n(H) = \{f(x) \in \mathcal{E}_n(H) : f(x+1) \in \mathcal{E}_n\}.$$

Then for $n \geq 2$,

$$\#\mathcal{F}_n(H) \leq (\tau_n + o(1)) (2H)^{n+1}.$$

Proof. Fix some sufficiently large H and let

$$f(x) = \sum_{i=0}^n a_i x^i \in \mathcal{E}_n(H).$$

Consequently,

$$f(x+1) = \sum_{i=0}^n A_i x^i,$$

with $A_i = a_i + L_i(a_n, a_{n-1}, \dots, a_{i+1})$ where $L_i(a_n, a_{n-1}, \dots, a_{i+1})$ is a linear form in $a_n, a_{n-1}, \dots, a_{i+1}$ for $i = 0, \dots, n$. In particular,

$$A_n = a_n, \quad A_{n-1} = na_n + a_{n-1}, \quad A_{n-2} = \frac{n(n-1)}{2}a_n + (n-1)a_{n-1} + a_{n-2}.$$

Clearly there are at most $O(H^n)$ polynomials $f \in \mathcal{I}_n(H)$ for which the condition

$$2A_{n-2} - (n-1)A_{n-1} = (n-1)a_{n-1} + 2a_{n-2} \neq 0. \quad (5)$$

is violated. Thus

$$\#\mathcal{F}_n(H) = \#\mathcal{F}_n^*(H) + O(H^n), \quad (6)$$

where $\mathcal{F}_n^*(H)$ is the set of polynomials $f \in \mathcal{F}_n(H)$ for which (5) holds.

Now, given two primes p and q , we calculate an upper bound on the number $N_n(H, p, q)$ of $f \in \mathcal{F}_n^*(H)$ such that

- $f(x)$ is irreducible by Eisenstein with respect to prime p ;
- $f(x+1)$ is irreducible by Eisenstein with respect to prime q .

We see from Lemma 6 that $N_n(H, p, q) = 0$ if $p = q$. So we now always assume that $p \neq q$.

To do so we estimate (inductively over $i = n, n-1, \dots, 0$) the number of possibilities for the coefficient a_i of f , provided that higher coefficients a_n, \dots, a_{i+1} are already fixed.

- Possible values of a_n : We know that $a_n \not\equiv 0 \pmod{p}$ and $a_n \not\equiv 0 \pmod{q}$. Therefore we conclude that the number of possible values of a_n is $2H(p-1)(q-1)/pq + O(1)$.
- Possible values of a_i , $1 \leq i < n$: Fix arbitrary $a_n, a_{n-1}, \dots, a_{i+1}$. The relations

$$a_i \equiv 0 \pmod{p} \quad \text{and} \quad A_i = a_i + L_i(a_n, a_{n-1}, \dots, a_{i+1}) \equiv 0 \pmod{q}$$

put a_i in a unique residue class modulo pq . It follows that the number of possible values of a_i for $i = n-1, n-2, \dots, 1$ cannot exceed $2H/pq + O(1)$.

- Possible values of a_0 : We argue as before but also note that for a_0 we have the additional constraints that $A_0 \not\equiv 0 \pmod{p^2}$, $a_0 \not\equiv 0 \pmod{q^2}$ and so a_0 can take at most $2H(q-1)(p-1)/p^2q^2 + O(1)$ values.

So, for primes p and q we have

$$\begin{aligned} N_n(H, p, q) &\leq \left(\frac{2H(p-1)(q-1)}{pq} + O(1) \right) \left(\frac{2H}{pq} + O(1) \right)^{n-1} \\ &\quad \left(\frac{2H(p-1)(q-1)}{p^2q^2} + O(1) \right) \\ &= \frac{2^{n+1}H^{n+1}(p-1)^2(q-1)^2}{p^{n+2}q^{n+2}} + O(H^n). \end{aligned}$$

We also see from (5) that if $pq > (n+1)H$ then $N_n(H, p, q) = 0$. Hence

$$\begin{aligned} \#\mathcal{F}_n^*(H) &\leq \sum_{\substack{p \neq q \\ pq \leq (n+1)H}} \left(\frac{2^{n+1}H^{n+1}(p-1)^2(q-1)^2}{p^{n+2}q^{n+2}} + O(H^n) \right) \\ &\leq (2H)^{n+1} \sum_{\substack{p \neq q \\ pq \leq (n+1)H}} \left(\frac{(p-1)^2(q-1)^2}{p^{n+2}q^{n+2}} \right) + O\left(\frac{H^{n+1} \log \log H}{\log H} \right), \end{aligned}$$

as there are $O(Q(\log Q)^{-1} \log \log Q)$ products of two distinct primes $pq \leq Q$, see [11, Chapter II.6, Theorem 4]. Therefore,

$$\#\mathcal{F}_n^*(H) \leq (2H)^{n+1} \sum_{\substack{p \neq q \\ pq \leq (n+1)H}} \frac{(p-1)^2(q-1)^2}{p^{n+2}q^{n+2}} + o(H^{n+1}),$$

Since the above series converges, we derive

$$\begin{aligned} \#\mathcal{F}_n^*(H) &\leq (2H)^{n+1} \sum_{p \neq q} \frac{(p-1)^2(q-1)^2}{p^{n+2}q^{n+2}} + o(H^{n+1}) \\ &= (2H)^{n+1} \left(\sum_{p,q} \frac{(p-1)^2(q-1)^2}{p^{n+2}q^{n+2}} - \sum_p \frac{(p-1)^4}{p^{2n+4}} \right) + o(H^{n+1}), \end{aligned}$$

which concludes the proof. \square

We can now prove the main result of this section. We recall that ρ_n and τ_n are defined by (3) and (4), respectively.

Theorem 8. *For $n \geq 2$ we have*

$$\liminf_{H \rightarrow \infty} \frac{\#\overline{\mathcal{E}}_n(H)}{\#\mathcal{E}_n(H)} \geq 1 + \gamma_n,$$

where

$$\gamma_n = \frac{1}{2^{n^2+n}} \left(1 - \frac{\tau_n}{\rho_n} \right) > 0.$$

Proof. We see from Lemma 4 that for $h = H/2^n$ we have

$$\mathcal{E}_n(H) \bigcup (\mathcal{E}_n(h) \setminus \mathcal{F}_n(h)) \subseteq \overline{\mathcal{E}}_n(H),$$

where $\mathcal{F}_n(h)$ is defined as in Lemma 7. Therefore, since $\mathcal{F}_n(h) \subseteq \mathcal{E}_n(h)$, we have

$$\#\overline{\mathcal{E}}_n(H) \geq \#\mathcal{E}_n(H) + \#\mathcal{E}_n(h) - \#\mathcal{F}_n(h).$$

Recalling Lemmas 5 and 7 we derive the desired inequality.

It now remains to show that $\gamma_n > 0$. So it suffices to show that

$$\rho_n - \tau_n > 0.$$

From (3) and (4) we have

$$\begin{aligned}
\rho_n - \tau_n &= 1 - \prod_p \left(1 - \frac{(p-1)^2}{p^{n+2}} \right) - \left(\sum_p \frac{(p-1)^2}{p^{n+2}} \right)^2 + \sum_p \frac{(p-1)^4}{p^{2n+4}} \\
&\geq 1 - \prod_p \left(1 - \frac{(p-1)^2}{p^{n+2}} \right) - \left(\sum_p \frac{(p-1)^2}{p^{n+2}} \right)^2 \\
&= \sum_{k=1}^{\infty} (-1)^{k+1} \sum_{p_1 < \dots < p_k} \prod_{j=1}^k \frac{(p_j-1)^2}{p_j^{n+2}} - \left(\sum_p \frac{(p-1)^2}{p^{n+2}} \right)^2.
\end{aligned}$$

Discarding from the first sum all positive terms (corresponding to odd k) except for the first one, we obtain

$$\begin{aligned}
\rho_n - \tau_n &\geq \sum_p \frac{(p-1)^2}{p^{n+2}} - \sum_{k=1}^{\infty} \sum_{p_1 < \dots < p_{2k}} \prod_{j=1}^{2k} \frac{(p_j-1)^2}{p_j^{n+2}} - \left(\sum_p \frac{(p-1)^2}{p^{n+2}} \right)^2 \\
&\geq \sum_p \frac{(p-1)^2}{p^{n+2}} - \sum_{k=1}^{\infty} \frac{1}{(2k)!} \left(\sum_p \frac{(p-1)^2}{p^{n+2}} \right)^{2k} - \left(\sum_p \frac{(p-1)^2}{p^{n+2}} \right)^2 \\
&\geq \sum_p \frac{(p-1)^2}{p^{n+2}} - \sum_{k=1}^{\infty} \left(\sum_p \frac{(p-1)^2}{p^{n+2}} \right)^{2k} - \left(\sum_p \frac{(p-1)^2}{p^{n+2}} \right)^2.
\end{aligned}$$

Hence, denoting

$$P_n = \sum_p \frac{(p-1)^2}{p^{n+2}},$$

we derive

$$\rho_n - \tau_n \geq P_n - \frac{P_n^2}{1 + P_n^2} - P_n^2.$$

Since

$$P_n \leq P_2 \leq 0.18,$$

the result now follows. \square

It is certainly easy to get an explicit lower bound on γ_n in Theorem 8. Various values of γ_n using the first 10,000 primes are given in Table 1.

Table 1: Approximations to γ_n for some n

| n | γ_n |
|-----|------------------------|
| 2 | 1.33×10^{-2} |
| 3 | 2.36×10^{-4} |
| 4 | 9.44×10^{-7} |
| 5 | 9.28×10^{-10} |
| 10 | 7.70×10^{-34} |

Question 9. Obtain tight bounds or the exact values of

$$\liminf_{H \rightarrow \infty} \frac{\#\overline{\mathcal{E}}_n(H)}{(2H)^{n+1}} \quad \text{and} \quad \limsup_{H \rightarrow \infty} \frac{\#\overline{\mathcal{E}}_n(H)}{(2H)^{n+1}}$$

(they most likely coincide).

5 Infinitude of $\mathcal{I}_n \setminus \overline{\mathcal{E}}_n$

We note that a consequence of Lemma 1 is that any polynomial belongs to $\mathcal{I}_n \setminus \overline{\mathcal{E}}_n$ if its discriminant is $n - 1$ free. Hence we would expect the size of $\mathcal{I}_n \setminus \overline{\mathcal{E}}_n$ to be “massive”. In fact, for a fixed degree greater than or equal to 2, we can prove that the number of irreducible polynomials that are not shifted Eisenstein polynomials is infinite.

Theorem 10. *The set $\mathcal{I}_n \setminus \overline{\mathcal{E}}_n$ is infinite for all $n \geq 2$.*

Proof. Let $f(x) = x^n + x + p$ for some $n \geq 2$ and even prime p . Then f is irreducible (see [9, Lemma 9]). Since no prime can divide the coefficient of x it follows that f is not an Eisenstein polynomial.

We show that f cannot be an Eisenstein shift polynomial. Suppose this is not the case. Then for some integer s the polynomial $f(x+s)$ is an Eisenstein polynomial with respect to some prime q . We have

$$f(x+s) = x^n + nsx^{n-1} + \dots + (ns^{n-1} + 1)x + s^n + s + p,$$

and so $ns \equiv 0 \pmod{q}$. If $s \equiv 0 \pmod{q}$, then as previously explained in the proof of Lemma 1, $f(x+s+kq)$ is an Eisenstein polynomial for any integer

k . Since f is not an Eisenstein polynomial it follows that $s \not\equiv 0 \pmod{q}$. So $n \equiv 0 \pmod{q}$. But then $ns^{n-1} + 1 \equiv 0 \pmod{q}$; a contradiction.

So we conclude that for any $n \geq 2$ the infinite set

$$\{f(x) = x^n + x + p : p \text{ an even prime}\}$$

consists of irreducible polynomials that are not shifted Eisenstein polynomials. \square

We also expect that

$$\lim_{H \rightarrow \infty} \frac{\#(\mathcal{I}_n \setminus \overline{\mathcal{E}}_n)}{\#\mathcal{I}_n} > 0.$$

For example, it is natural to expect that there is a positive proportion of polynomials \mathcal{I}_n with a square-free discriminant, which by Lemma 1 puts them in the set $\mathcal{I}_n \setminus \overline{\mathcal{E}}_n$. However, even the conditional (under the *ABC*-conjecture) results of Poonen [10] about square-free values of multivariate polynomials are not sufficient to make this claim.

We can however prove an inferior result, for degrees greater than 2, involving height constrained polynomials that can be shifted to a height constrained Eisenstein polynomial.

Theorem 11. *Let*

$$\overline{\mathcal{C}}_n(H) = \{f(x) \in \overline{\mathcal{E}}_n(H) : f(x+s) \in \mathcal{E}_n(H) \text{ for some } s \in \mathbb{Z}\}.$$

Then for $n > 2$,

$$\lim_{H \rightarrow \infty} \frac{\#\overline{\mathcal{C}}_n(H)}{2H(2H+1)^n} < 1.$$

Proof. Let $\overline{\mathcal{C}}_n(d, H)$ be the set of all polynomials

$$f(x+s) = a_n(x+s)^n + a_{n-1}(x+s)^{n-1} + \dots + a_1(x+s) + a_0 \in \mathbb{Z}[x]$$

such that:

- (i) $s \in \mathbb{Z}$,
- (ii) $H(f(x+s)) \leq H$,
- (iii) $f(x)$ is Eisenstein with respect to all the prime divisors of d ,

$$(iv) \ H(f(x)) \leq H,$$

$$(v) \ |s| < d.$$

Note that each element of $\overline{\mathcal{C}}_n(d, H)$ may come from several pairs (f, s) .

We also observe that the set of all $f(x)$ described in (iii) and (iv) is precisely $\mathcal{H}_n(d, H)$, where $\mathcal{H}_n(d, H)$ is the set of polynomials (1) of height at most H and such that

$$(a) \ d \mid a_i \text{ for } i = 0, \dots, n-1,$$

$$(b) \ \gcd(a_0/d, d) = 1,$$

$$(c) \ \gcd(a_n, d) = 1.$$

It then follows from the condition (v) in the definition of $\overline{\mathcal{C}}_n(d, H)$ that

$$\#\overline{\mathcal{C}}_n(d, H) \leq 2d\#\mathcal{H}_n(d, H).$$

Using the inclusion exclusion principle implies that

$$\#\overline{\mathcal{C}}_n(H) \leq \sum_{\substack{2 \leq d \leq H \\ \mu(d) = -1}} \#\overline{\mathcal{C}}_n(d, H),$$

and so

$$\#\overline{\mathcal{C}}_n(H) \leq \sum_{\substack{2 \leq d \leq H \\ \mu(d) = -1}} 2d\mathcal{H}_n(d, H). \quad (7)$$

From [6], we have

$$\mathcal{H}_n(d, H) = \frac{2^{n+1}H^{n+1}\varphi^2(d)}{d^{n+2}} + O\left(\frac{H^n}{d^{n-1}}2^{\omega(d)}\right). \quad (8)$$

Combining (7) and (8) we have

$$\begin{aligned} \#\overline{\mathcal{C}}_n(H) &\leq \sum_{\substack{2 \leq d \leq H \\ \mu(d) = -1}} 2d \left(\frac{2^{n+1}H^{n+1}\varphi^2(d)}{d^{n+2}} + O\left(\frac{H^n 2^{\omega(d)}}{d^{n-1}}\right) \right) \\ &= 2 \sum_{\substack{2 \leq d \leq H \\ \mu(d) = -1}} \left(\frac{2^{n+1}H^{n+1}\varphi^2(d)}{d^{n+1}} + O\left(\frac{H^n 2^{\omega(d)}}{d^{n-2}}\right) \right). \end{aligned}$$

Hence

$$\begin{aligned} \frac{\#\bar{\mathcal{C}}_n(H)}{2H(2H+1)^n} &\leq 2 \sum_{\substack{2 \leq d \leq H \\ \mu(d)=-1}} \left(\frac{\varphi^2(d)}{d^{n+1}} + O\left(\frac{2^{\omega(d)}}{Hd^{n-2}}\right) \right) \\ &= 2 \sum_{\substack{2 \leq d \leq H \\ \mu(d)=-1}} \frac{\varphi^2(d)}{d^{n+1}} + O\left(\frac{1}{H} \sum_{2 \leq d \leq H} \frac{2^{\omega(d)}}{d^{n-2}}\right) \end{aligned}$$

for all $n > 2$. It's easy to see that

$$\sum_{d=2}^H \frac{2^{\omega(d)}}{d^{n-2}} = o(H)$$

for all $n > 2$. Hence

$$\frac{\#\bar{\mathcal{C}}_n(H)}{2H(2H+1)^n} \leq 2 \sum_{\substack{2 \leq d \leq H \\ \mu(d)=-1}} \frac{\varphi^2(d)}{d^{n+1}} + o(1).$$

So

$$\begin{aligned} \lim_{H \rightarrow \infty} \frac{\#\bar{\mathcal{C}}_n(H)}{2H(2H+1)^n} &\leq 2 \sum_{\mu(d)=-1} \frac{\varphi^2(d)}{d^{n+1}} \leq 2 \sum_{\mu(d)=-1} \frac{1}{d^{n-1}} = 2 \sum_{k=0}^{\infty} \sum_{\omega(d)=2k+1} \frac{1}{d^{n-1}} \\ &\leq 2 \sum_{k=0}^{\infty} \left(\frac{1}{(2k+1)!} \left(\sum_p \frac{1}{p^{n-1}} \right)^{2k+1} \right) \\ &\leq 2 \sinh \left(\sum_p \frac{1}{p^{n-1}} \right) \leq 2 \sinh \left(\sum_p \frac{1}{p^2} \right). \end{aligned}$$

As direct calculations show that

$$\sum_p \frac{1}{p^2} < 0.46,$$

the result follows. □

We infer from [1, Theorem 1] that

$$\lim_{H \rightarrow \infty} \frac{\#\mathcal{I}_n(H)}{2H(2H+1)^n} = 1,$$

which when combined with Theorem 11 yields

$$\lim_{H \rightarrow \infty} \frac{\#(\mathcal{I}_n(H) \setminus \overline{\mathcal{C}}_n(H))}{\#\mathcal{I}_n(H)} > 0,$$

for $n > 2$.

6 Some numerical results

As we have mentioned, we believe that the upper and lower limits in Question 9 coincide and so the density of shifted Eisenstein polynomials can be correctly defined.

By using Monte Carlo simulation we have calculated approximations to the values of $\#\mathcal{E}_3(H)$ and $\#\overline{\mathcal{E}}_3(H)$ which suggests that $\#\overline{\mathcal{E}}_3(H)/\#\mathcal{E}_3(H)$ is about 3, see Table 2.

Table 2: Monte Carlo Experiments for Cubic Polynomials

| | |
|---------------------------------|-------------|
| Maximum height of polynomials: | 1, 000, 000 |
| Number of simulations: | 20, 000 |
| Shifted Eisenstein polynomials: | 1, 119 |
| Eisenstein polynomials: | 3, 365 |
| Ratio: | 3.0 |

For quartics polynomials the ratio $\#\overline{\mathcal{E}}_4(H)/\#\mathcal{E}_4(H)$ is approximately 3.6 as shown in Table 3.

Table 3: Monte Carlo Experiments for Quartic Polynomials

| | |
|---------------------------------|-------------|
| Maximum height of polynomials: | 1, 000, 000 |
| Number of simulations: | 20, 000 |
| Shifted Eisenstein polynomials: | 1515 |
| Eisenstein polynomials: | 419 |
| Ratio: | 3.6 |

7 Comments

It is easy to see that the results of the work can easily be extended to monic polynomials.

We note that testing whether $f \in \mathcal{E}_n$ can be done in an obvious way via several greatest common divisor computations. We however do not know any efficient algorithm to test whether $f \in \overline{\mathcal{E}}_n$. The immediate approach, based on Lemma 1 involves integer factorisation and thus does not seem to lead to a polynomial time algorithm. It is possible though, that one can get such an algorithm via computing greatest common divisor of pairwise resultants of the coefficients of $f(x + s)$ (considered as polynomials in s).

We also note that it is interesting and natural to study the *affine Eisenstein polynomials*, which are polynomials f such that

$$(cx + d)^n f\left(\frac{ax + b}{cx + d}\right) \in \mathcal{E}_n$$

for some $a, b, c, d \in \mathbb{Z}$. Studying the distribution of such polynomials is an interesting open question.

8 Acknowledgment

The authors would like to acknowledge the assistance of Hilary Albert with the programming for Section 6.

This work was supported in part by the ARC Grant DP130100237.

References

- [1] S. D. Cohen, ‘The distribution of the Galois groups of integral polynomials’, *Illinois Journal of Mathematics*, **23** (1979), 135–152.
- [2] D. A. Cox, ‘Why Eisenstein proved the Eisenstein criterion and why Schonemann discovered it first’, *Amer. Math. Monthly*, **118** (2011), 3–21.
- [3] R. Dietmann, ‘On the distribution of Galois groups’, *Mathematika*, **58** (2012), 35–44.

- [4] D. E. Dobbs and L. E. Johnson, ‘On the probability that Eisenstein’s criterion applies to an arbitrary irreducible polynomial’, *Proc. of 3rd Intern. Conf. Advances in Commutative Ring Theory*, Fez, Morocco, Lecture Notes in Pure and Appl. Math., **205**, Dekker, New York, 1999, 241–256.
- [5] A. Dubickas, ‘Polynomials irreducible by Eisenstein’s criterion’, *Appl. Algebra Engin. Comm. Comput.*, **14** (2003), 127–132.
- [6] R. Heyman and I. E. Shparlinski, ‘On the number of Eisenstein polynomials of bounded height’, *Preprint*, 2012.
- [7] A. K. Lenstra, H. W. Lenstra and L. Lovász, ‘Factoring polynomials with rational coefficients’, *Mathematische Annalen*, **261** (1982), 515–534.
- [8] K. Mahler, ‘An inequality for the discriminant of a polynomial’, *Michigan Math. J.*, **11** (1964), 257–262.
- [9] H. Osada, ‘The Galois groups of the polynomials $x^n + ax^l + b$ ’, *J. Number Theory*, **25** (1987), 230–238.
- [10] B. Poonen, ‘Squarefree values of multivariable polynomials’, *Duke Math. J.*, **118** (2003), 353–373.
- [11] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, 1995.
- [12] D. Zywina, ‘Hilbert’s irreducibility theorem and the larger sieve’, *Preprint*, 2010 (available from <http://arxiv.org/abs/1011.6465>).